情報家電のセキュリティ向上に向けて

2010年度版
情報家電におけるセキュリティ対策
検討報告書

■ 情報家電のセキュリティにおける課題と解決の方向性

■ デジタルテレビにおけるセキュリティ対策検討ガイド

・セキュリティ対策 テンプレート／チェックリスト

2011年1月

独立行政法人 情報処理推進機構

<目次>

<図表目次>

１．　はじめに

1.1　背景、課題および解決のアプローチ

組込み機器のネットワーク接続が急激に増加してきて、利用形態にも大きな変化が起き始めている。情報家電もその一つで、家電がネットワークにつながるようになって利用できる機能や利便性が増し、メーカーにとっても新たな事業拡大の兆しが出てきている。その一方で、以下のような、セキュリティ対応への懸案、課題が浮上してきている：

１）セキュリティ脅威の増大：　汎用部品や汎用ソフトの活用、TCP/IP や無線 LAN といった標準の通信プロトコルの活用により、情報セキュリティ面での脅威が大幅に増加してきている。家電がＰＣと同じ環境に近付いてきており、ＰＣで起っている脅威が情報家電でも起こりうる状況になってきている。

２）セキュリティ対策への取組み：　セキュリティ対策（費用負担を含む）は誰（利用者、メーカー）が、どのレベルまで実施するべきか、またセキュリティ事故（インシデント）の発生時にどう対策を徹底するのか、など、業界および市場での共通認識が確立していない。

３）利用者のリテラシー・意識向上：　利用者のセキュリティ教育やリテラシー向上をどう実現するのかなど、これまでの家電の常識、家電に対する利用者の意識の変革やコンセンサスの醸成が不可欠となってきている。

こうした背景を受け、（独）情報処理推進機構（IPA）では、家電業界各社とオブザーバとして経済産業省（METI）の参画のもとに、2010 年３月より 12 月にかけて計７回の勉強会を実施した。その目的は、今後普及が進んでいくネットワークに接続される情報家電において、想定されるセキュリティ上の課題の明確化と共有化を行い、メーカーと利用者と制度面の三位一体の下で、新しい市場の形成および発展に寄与することを目的としている。

1.2　本報告書の概要と位置づけ

本報告書は、その勉強会で明らかになった懸案事項、隘路、課題、その解決の方向性、提言と、デジタルテレビを具体的な対象としてセキュリティ対策をまとめたものである。

第２章は、情報家電全般に対して、懸念事項、セキュリティ対策の課題、解決の方向性をまとめたものである。

第３章は、既に先行製品が出始めており、今後益々市場が拡大していくものと想定されるインターネットに接続されるデジタルテレビに対象を絞って、より具体的に、想定される脅威、セキュリティ対策の検討を行ったものである。機能から脅威、対策を網羅的・ニュートラルに洗い出したものであり、各社の製品には既にとり込まれている対策もあるものと考えられるが、今後、確立が望まれる共通のセキュリティ基準（標準）を検討していく上で、考えうる対策の

母集団として基礎になることを期待している。

IPA では、2005 年度より組込みシステムにおけるセキュリティ対策が今後重要な課題になるとの認識の下、調査研究やガイドの策定を推進してきている（IPA 公開 Web :【調査報告書】組込みシステム・制御システム　参照[1]）。 その中で、本報告に特に関連の深いものとして、以下が挙げられるので、合わせて参照頂きたい。

・「組込みシステムのセキュリティへの取組みガイド（改訂版）」[2]：

　システムや機器開発にあたって、セキュリティへの取り組みは、メーカーにとって大きな課題となってくる。これに対しては、組織のマネジメント、および各開発フェーズ（企画、開発、運用、廃棄）におけるセキュリティへの取り組みに関するガイドである。

・「組込みソフトウェアを用いた機器におけるセキュリティ」[3]：

　組込み機器の利用における事故事例やセキュリティ対策の取組みの全体概要について解説している。

これらに対して、本報告書は、情報家電、特にデジタルテレビを対象に、どのような脅威が存在し、それに対するセキュリティ対策を具体的に示したものである。商品の企画、開発フェーズで、搭載すべきセキュリティ機能を検討、設計する際に参照頂くことを想定している。また、搭載すべきセキュリティ機能のテンプレートやセキュリティ対策のチェックリストとして活用頂けることを目標としている。

今後、本報告書の３章「デジタルテレビに対するセキュリティ対策検討ガイド」に関しては、定期的な更新が必要である。

1.3　設置した勉強会の出席者一覧

2010 年 3 月より 12 月にかけて計 7 回の勉強会を実施した。以下、出席頂き、掲載許可頂いた方々です。

所属	氏名（敬称略）
シャープ株式会社	石川　則夫
	大久保　琢也
	稗田　薫
	田中　敏幸
ソニー株式会社	森田　直
	小林　正和
パナソニック株式会社	冨田　克彦
	再起　和夫
日立コンシューマエレクトロニクス株式会社	山田　佳弘
三菱電機株式会社	藤城　直
経済産業省　商務情報政策局 情報セキュリティ政策室 ＜オブザーバ＞	清水　友晴
	納屋　知佳
	佐藤　明男
IPA　セキュリティセンター	矢島　秀浩
	小林　偉昭
	金野　千里
	中野　学
	長谷川　智香
	萱島　信
	鵜飼　裕司

２．情報家電のセキュリティにおける課題と解決の方向性

今年から、家電をインターネットに接続して、外部へのアクセスや外部からの制御などの便利な機能の話題が挙がってきたが、セキュリティ上の脆弱性をついた外部からの攻撃や、情報漏えいなどの脅威も想定され、インターネットに接続された製品や機能がまだ一部の用途に留まっているのが現状である。

こうした背景を受け、本章では、2010 年における情報家電のセキュリティに対する課題、懸案事項を纏める。

2.1　情報家電のセキュリティ上の課題

本勉強会で議論した情報家電の市場が普及、拡大していくためのセキュリティ上の課題を整理すると、以下の四つの観点からなる：

(1)　脅威の共通認識とセキュリティ対策の必要性

脅威は、機能利用の妨害や情報漏えいなど、損失（リスク）を引き起こす攻撃手段であり、機能が増えればそれに応じて脅威も増えていく。脅威だけではリスクが起きる訳ではないが、想定される脅威を洗い出し、それを受けてしまう脆弱性の対策をしたり、脅威自体に対するセキュリティ対策を予め打っておくことは、リスクを低減する上で非常に重要となる。

① 脅威の共通認識

・プラットフォームに汎用部品が使われてきており、任意コードの実行といった深刻な脅威も高まっている。

・情報家電がネットワークアクセスを含め、PC の環境に近付いており、PC で起っている脅威と同等の脅威に晒される恐れがある。

・製品の脆弱性対策を含めたアップデートには期間的な限界（プラットフォームのサポート期限等）があるが、家電の 10～15 年におよぶ長期間利用にどう対応していくか。

②業界の懸案、隘路

・メーカーとして、外部からくる脅威に対してまで、製品の安心、安全をどの程度、宣言できるのか。

・情報セキュリティに起因した事故時、メーカーの責任範囲のコンセンサスが必要となる。

・設定ミスなどもセキュリティの脅威になるため、マニュアル、取扱説明書の記載レベルの基準が必要である。

③方向性：　セキュリティ基準、ガイドライン、認証

・業界で決めたセキュリティ対策上の基準的なものがあって初めて、ユーザも含めて不安が払拭される。

・セキュリティ対策や脆弱性対応や暗号アルゴリズム選定のチェックリストなどの、合意されたガイドラインが必要である。

・基準もしくはガイドラインを満たしていることを、中立機関で認証するという仕掛けがあると望ましいが、極力コスト（認定期間含む）がかからない考慮が必要である。

(2)　情報家電市場形成の必要性

①ユーザの状況

・安全との認識の強い家電において、起りうるセキュリティの脅威が一般消費者に理解して頂くのが困難である。

・PC はセキュリティ対策が必須という市場形成がなされてきているが、情報家電の利用者層はそれより広範となる。

・情報家電に対するセキュリティ意識は行き渡っておらず、どう説明、理解してもらい、リテラシーの向上を図るかが課題である。

・安全な筈の製品に何故セキュリティ対策でお金をかけるのか、なかなか理解が得られない。

②機器の利用面の隘路

・取扱説明書には沢山書いてきているが、機器を正しく設定してもらえるかが課題である。

・情報家電で何か起った時、どうすれば良いのか、機能利用だけでなくユーザのセキュリティ対応面などに対するリテラシーの向上が重要である。

③事故・故障対応

・事故や故障の原因として、設定不良、ネット接続利用、改造や機能追加など様々考えられ、その切り分けが困難であり、またユーザとの責任分界点の明確化が必要である。

・ユーザは攻撃にあっていることや、自身が（踏み台等で）加害者になっていることに気付かないケースへの対応も必要である。

・脆弱性をついた攻撃は、利用者だけでなくメーカーともに被害者であり、その対応の枠組み（攻撃者の特定や事後対応など）を整備する必要がある。

④方向性：　市場形成

・各社で個別にネット接続の注意事項、危険性をユーザに説明するのは難しく、業界で纏まったものが必要である。

・製品品質と脆弱性は本質的に異なっており、脆弱性を狙った害意のある第三者による攻撃で起きた事故をどう捉えるか、市場としての共通認識が必要である。脆弱性とは、ソフトウェア製品やアプリケーションシステム等において、不正アクセスやコンピュータウイルス等の攻撃により、その機能や性能を損なう原因となりえる箇所のことである[7]。

(3)　業界としての連携、情報共有の必要性

①業界としての連携

・ネット接続に伴う危険性を各社が個別で出すのは難しく、業界で纏められることが望ましい。

・脆弱性のレベルが軽微か、重大かの判断を各社がするのは難しく、共通の尺度が必要である。

②情報共有の必要性

・攻撃事例の共有、継続的に議論できる場や体制が必要である。

・脅威情報、脆弱性情報など、業界で共有できるニュートラルな DB が必要である。　DB は、開発者向けと、ユーザ向けのそれぞれのものが必要である。

(4)　市場の牽引と発展

①市場の牽引

・世界市場でコスト、機能における競争の中で、コスト優先でセキュリティ対策レベルが低い情報家電が市場に出回るのは、ユーザにとっても、市場形成からも好ましくない。

・海外 OEM 生産品の使用が増える方向であるので、それらにどのような受入れ検査をすればよいかも課題となる。

②国際標準、認証

・セキュリティ基準を ISO 等に提案して、それをクリアした、あるいは認証を受けた製品が消費者に選択される市場の流れを作るのが望ましい。

2.2　情報家電セキュリティの解決の方向性

前 2.1 節で挙げた課題、懸案事項に対し、その解決の方向性として、今後、

(1) 情報家電セキュリティ基準の確立

(2) マーケットの育成、情報家電リテラシーの向上

(3) 情報ＤＢの整備

(4) グローバルデファクト、国際標準への展開

などの各項目への取り組みが必要であるとの結論を得た。

表 1 に、前 2.1 節で挙げた課題、懸案事項と、本節で述べるその解決の方向性の関連の一覧を示す。

以下、解決の方向性で挙げた各項目に対して、本勉強会での議論を纏めた要件内容を記載する。なお、勉強会の中での議論内容や補足情報について、注)として付記する。

（１）情報家電セキュリティ基準の確立

業界として準拠すべきセキュリティ基準の確立が望まれる。この基準が、メーカーとしての責任範囲の社会的コンセンサスとなることも期待したい。ただし、対象製品分野や利用機能範囲によって脅威や影響範囲がかなり異なるので、製品分野ごとの基準が必要である。

①　情報家電セキュリティ基準

製品分野や利用機能範囲（レベル）毎に、以下を規定する：

・保護すべき資産 [注1)] および脅威の明確化

・製品へのセキュリティ対策実装項目（利用機能によるレベル、段階が必要）

・製造現場におけるセキュリティ管理体制

・製品取扱い説明書への記載事項、記載レベル

・発売後の運用スキーム（脆弱性対策など）

・新しい技術（IPv6 等）への対応

表１．情報家電の課題と解決の方向性

#	課題			解決の方向性	
	分　類	小項目		対応項目	目　標
1	脅威の共通認識 と セキュリティ対策の 必要性	＜脅威＞ ・プラットフォームに汎用部品が使われてきており、任意コードの実行といった深刻な脅威も高まっている。 ・情報家電がネットワークアクセスを含め、PCの環境に近付いており、PCで起っている脅威と同等の脅威に晒される恐れがある。 ・製品の脆弱性対策を含めたアップデートには期間的な限界（プラットフォームのサポート期限等）があるが、家電の10～15年におよぶ長期間利用にどう対応していくか。		情報家電 セキュリティ基準	情報家電 セキュリティ基準 の確立
		＜業界の隘路・懸案＞ ・企業として、外部からくる脅威に対してまで、製品の安心、安全をどの程度、宣言できるのか。 ・情報セキュリティに起因した事故時、メーカーの責任範囲のコンセンサスが必要となる。 ・設定ミスなどもセキュリティの脅威になるため、マニュアル、取扱説明書の記載レベルの基準が必要である。			
		＜方向性：　セキュリティ基準、ガイドライン、認証＞ ・業界で決めたセキュリティ対策上の基準的なものがあって初めて、ユーザも含めて不安が払拭される。 ・セキュリティ対策や脆弱性対応や暗号アルゴリズム選定のチェックリストや合意されたガイドラインが必要である。 ・中立機関による認証という仕掛けがあると望ましいが、極力コスト（認定期間含む）がかからない考慮が必要である。		認証・認定制度	
2	情報家電 市場形成 の必要性	＜ユーザ状況＞ ・安全との認識の強い家電において、起りうるセキュリティの脅威が一般消費者に理解して頂くのが困難である。 ・PCはセキュリティ対策が必須という市場形成がなされてきているが、情報家電のユーザー層はそれより広範となる。 ・情報家電に対するセキュリティ意識は行き渡っておらず、どう説明、理解してもらい、リテラシーの向上を図るかが課題である。 ・安全な筈の製品に何故セキュリティ対策でお金をかけるのか、なかなか理解が得られない。		ネット接続機能利用で想定される脅威の理解	製品ライフサイクルへの対応 マーケット の育成 （ベンダー） ・ リテラシー の向上 （ユーザ）
		＜機器の利用面の隘路＞ ・取扱説明書には沢山書いてきているが、機器を正しく設定してもらえるかが課題である。 ・情報家電で何か起った時、どうすれば良いのか、機能利用だけでなくユーザのリテラシーの向上が重要である。		ユーザ意思による機能選定の認識	
		＜事故・故障対応＞ ・事故や故障の原因として、設定不良、ネット接続利用、改造や機能追加など様々考えられ、その切り分けが困難であり、またユーザとの責任分界点の明確化が必要である。 ・ユーザーは攻撃にあっていることや、自身が（踏み台等で）加害者になっていることに気付かないケースもある。		利用時（廃棄フェーズも含む）の留意事項の徹底	
		＜方向性：　市場形成＞ ・各社で個別にネット接続の注意事項、危険性をユーザに説明するのは難しく、業界で纏まったものが必要である。 ・製品品質と脆弱性は本質的に異なっており、脆弱性が原因でおきた事故をどう捉えるか、共通認識が必要である。		事故発生時の対応フローの 整備・周知	
3	業界としての連携、 情報共有の必要性	＜業界としての連携＞ ・ネット接続に伴う危険性を各社が個別で出すのは難しく、業界で纏められることが望ましい。 ・脆弱性のレベルが軽微か、重大かの判断を各社がするのは難しく、共通の尺度が必要である		開発者向け情報 DB	情報DB の整備
		＜情報共有の必要性＞ ・攻撃事例の共有、継続的に議論できる場や体制が必要である。 ・脅威情報、脆弱性情報など、業界で共有できるニュートラルなDBが必要である。 DBは、開発者向けと、ユーザー向けのそれぞれのものが必要である。		ユーザ向け情報 DB	
4	市場の牽引 と発展	＜市場の牽引＞ ・世界市場でコスト、機能における競争の中で、コスト優先でセキュリティ対策レベルが低い情報家電が市場に出回るのは、ユーザにとっても、市場形成からも好ましくない。 ・海外OEM生産品の使用が増える方向であるので、それらにどのような受入れ検査をすればよいかも課題となる。		セキュリティ基準 の国際標準化	グローバル デファクト・ 国際標準化 への展開
		＜国際標準、認証＞ ・セキュリティ基準をISO等に提案して、それをクリアした、あるいは認証を受けた製品が消費者に選択される市場の流れを作るのが望ましい。		認証、認定制度 の 市場デファクト化	

利用機能によって、セキュリティレベルを選択できる体系が必要である[注2)]。

製品分野として、市場が先行しているデジタルテレビ（以下 DTV）を対象とした基準から着手するのがよいと考える。

なお、業界によるセキュリティ基準の先行事例としては、クレジットカード利用業界のセキュリティ基準である PCI DSS(Payment Card Industry Data Security Standard)[6】] が挙げられ、具体的な基準規定レベルなどで参考になる。

注 1） 保護すべき資産の定義として、情報家電機器、その機器に提供されるサービスフレームワーク（例えば専用ポータルサイト）など、対象範囲の特定が重要となる。また、保護すべき資産には、機器の利用で機器側に蓄積されるユーザの情報資産（例えば個人情報、知財権のあるコンテンツ）なども挙げられるので、その特定が重要である。

注 2） 利用機能として、大きくは、ネット接続未使用、特定の信頼できる接続先のみ許可、任意のサイトに接続許可、の３つのレベルに分けられる。例えば DTV では、

A. 従来タイプのネットワーク接続が出来ないテレビ

B. 信頼できるサーバ（原則テレビの提供メーカー運営）と一体となったインターネット安心テレビ

C. パソコンと同じようにインターネット接続がユーザ責任のパソコンタイプテレビ

の３つの形態が挙げられる。

また、ネット利用形態として、有線、無線があり、脅威や考慮しなくてはならないセキュリティ上の課題が異なってくる。それぞれに対して、実装すべきセキュリティ対策項目や、利用時の運用スキームを規定する必要がある。

② 認証・認定制度[注3)]

基準準拠を普及、推進する仕掛けとして、以下が要件となる：

・家電業界の事業環境（世界競合、製品長寿命、新製品短期開発サイクル等）に適合
・コスト負担や審査プロセスが過負荷にならない形態
・それぞれの規模の事業者の事業展開に負担が大き過ぎない形態
・製品の実情（機能レベルや市場規模等）を反映し、共通ルール（基準をベースとしたチェックリスト等）に基づいた自己宣言から、認証、認定シール貼付などのレベルの設定
・中立の第三者機関による認証・認定制度
・製品の価値（信頼性、安全性等）として、認定取得の意味が消費者に分かりやすい事

注 3） ある定められたセキュリティ基準に沿ってそれに準拠していることを評価、認証するもので、その基準が想定してない将来的に発生する未知の脅威にもセキュリティを保証するものではない。そのことを、利用者側でも、理解、認識する必要がある。

（２）マーケットの育成、情報家電リテラシーの向上

家電という固定観念／先入観（安全、常時稼働、ユーザメンテナンス不要など）に対して、以下に挙げる項目を浸透させる仕掛けが必要である。また、これによって、情報家電に対する責任分界点の社会共通認識が醸成されることが望まれる。

以下、製品の理解、利用、廃棄、事故対応などの製品ライフサイクルに沿って必要事項を述べる。

①　ネット接続機能利用で想定される脅威の理解

ネット接続機能（宅内LAN、インターネット）の利用や外部メディアの利用で、PCと変わらない脅威が発生しうることを、情報家電も想定する必要がある。一方、情報家電の利用者は全ての人が対象となることを考慮し、そうした脅威を周知していく取組みが重要であり、以下のような利用者へのアプローチが挙げられる：

・取扱説明書での記載内容(機能の利用と想定脅威の明記)
・パンフレット（広く周知させるための素材）
・公開Webサイト、教育素材

②　ユーザ意思による機能選定の認識

機能利用の必要性および想定される脅威を認識した上で、ユーザ意思（責任の一端）[注4)]で機能選択（機能活性化）をする共通認識が醸成される仕掛けが必要である：

・取扱説明書の記載内容およびレベルの規約（危険性、遵守事項、利用時対策などの記載）
・搭載機能の活性化の意思表示手段のルール化（例えば専用サイトでの登録、活性化など）

注4）ユーザ意思の確認には、機能や規約内容がよく理解できる説明とし、理解が不充分な中で安易にOKを押下（もしくは承諾）してしまわないための考慮が必要である。

③　利用時（廃棄フェーズ含む）の留意事項の徹底

ネット利用時に順守しなければならない事項を周知、徹底する仕掛けが必要である：

・セキュリティアップデートの必要性の理解（上記②の取扱説明書での記載）と運用
・ネット利用時に、アップデートへの誘導が図られるシステム仕様、あるいは強制する仕掛け（専用Web（Trusted home）の経由など）などの組み込みも選択肢の一つ[注5)]
・廃棄時、機器上に残る情報消去手段の提示

注5）具体的な仕掛けの事例として、以下が挙げられる：

・北米ではPull型のリモートメンテナンスが積極的に使われているが、日本は消極的。
・デジタルチューナーの付いている機器であれば、放送波の隙間で自動アップデートするルートが使われるが、電源が入っている必要がある。

・ゲーム機では、ネット経由でバージョンアップしないとサービスを受けられない仕組みとしており、強制的にアップデートを実現している。
・携帯電話は、キャリアが統括して機器管理（トレース)、パッチあてなどを管理している。

④ 事故発生時の対応フローの整備

情報家電におけるセキュリティ事故発生時に備えた以下の整備が挙げられる：
・取扱説明書での記載内容の規約
・問合せ窓口
・対応するＷｅｂサイトの設置

（３）情報ＤＢの整備

脆弱性対策情報、事件・事故に対して、対応する情報ＤＢとして、製品開発者が活用するＤＢと、製品利用者が活用できる２種類のＤＢの整備、活用できる仕掛けが必要である。
前者は上述の（１）と、後者は（２）と密接に関連してくる。

①　開発者向け情報ＤＢ

製品に対しては、共通のプラットフォームが部品として活用されていく傾向にあることから、国内の脆弱性対策情報データベースである JVN iPedia [4] [5] の活用が候補となる。但し、組込み系機器や情報家電の開発現場での利用を推進するために、情報収集対象の拡大や使い勝手（Ｉ/F）の向上などの検討が必要である [注6)]。

注 6）現行の JVN(Japan Vulnerability Note)[4] [5] の利用状況や利用現場の声を踏まえ、かつ情報家電に向けた検討が必要：
・オープンソースを使うケースが増えているが、JVN への届出は少ない。
・部品メーカーから直接情報を入手しているケースがある。

②　ユーザ向け情報ＤＢ

個別の製品に対するものは、各社の Web サイトで必要に応じて公開されるものと考える。PC やスマートフォンでの攻撃事例などをベースに、情報家電でも起こりうる攻撃の情報を揃えていく必要がある。一般消費者に認知され、理解し易く、アクセスが簡単な業界共通のユーザ向け DB の整備が必要である。
・情報家電全般もしくは製品分野共通の脆弱性や脅威
・注意喚起すべき事件・事故事例
・インシデント対応ノウハウ

（４）グローバルデファクト・国際標準への展開

情報家電の立ち上がりのこの時期に、セキュリティ基準の先行策定、国際標準化の流れを作

ることが考えられる。

①　セキュリティ基準の国際標準化

　メーカーがセキュリティ基準を策定し、それに準拠することにより、デファクトを確立し、国際標準にもっていく可能性を探ることが考えられる。

② 認証、認定制度の市場デファクト化

　グローバルデファクトへの展開として、以下が考えられる：

・認証を受けた製品が、消費者に選ばれるという土壌、流れを作っていく。
・消費者が安心できるセキュリティ対策により、高付加価値機能の先行開発に着手していける基盤を整備する。

３．デジタルテレビにおけるセキュリティ対策検討ガイド

本章では、より具体的に、デジタルテレビ（DTV）を対象に、前章で挙げた「セキュリティ基準」に対するアプローチの議論を報告する。機能から、想定される脅威、それに対する対策を、網羅的に洗い出したものであり、個々の製品に必要なセキュリティ対策や対策基準を策定するための基礎情報として活用されることを期待している。

デジタルテレビには、従来のテレビに較べて、外部メディア利用、内蔵ディスク、LAN 接続、インターネット接続など、様々な情報利用機能が付加されてきており、PC で起っている脅威と同じ事が起こる事が想定される。

付加される情報利用機能によって、新たな脅威が顕在化し、それに対する対策が必要となってくる。従って、一括りにデジタルテレビといっても、搭載されている情報利用機能によって、必要となるセキュリティ対策は大きく異なってくる。そこで、情報利用機能　→　想定される脅威　→　必要となるセキュリティ対策　の全体の相関を明確にするアプローチをとる。まず、3.1 節で情報利用機能群、3.2 節で想定されるセキュリティ脅威群、3.3 節でセキュリティ対策群を列挙し、3.4 節でそれらの対応、相関を、表２を用いて纏める。

3.1　デジタルテレビにおける情報利用機能

図１に、DTV における機能の全体構成図（概念図）を示す。本図では、放送を利用する従来のテレビの機能を家電機能（AV 機能部）、インターネットやメディアを利用した新たにデジタルテレビとして追加される機能を PC 機能（情報機能部）と、一義的に名称づけしている。

以下では、従来のテレビに追加される情報利用機能を説明する。　なお、従来のテレビ機能（映像受信、表示機能、利用管理機能等）を表２では基本機能としている。

＜→：表２下半分左欄の機能の項番に対応＞

⑴ 外部メディア利用機能

① 内蔵ドライブ　＜→　A1＞

DVD 等を読み込むオプティカルドライブである。

② 汎用インタフェース　＜→　A2＞

USB（Universal Serial Bus）や Ethernet など、汎用の外部接続インタフェース経由のメディア接続である。

⑵ 蓄積メディア内蔵　＜→　B＞

内蔵されている HDD（Hard Disk Drive）である。

(3) LAN 接続

① 有線 LAN　　　＜→　C1＞

IEEE802.3X(Ethernet)、PLC（Power Line Communication）などを介した家庭内の有線 LAN である。家庭内の他のメディア機器、プリンタ、PC などとの接続が想定される。

② 無線 LAN　　　＜→　C2＞

IEEE802.11X、Bluetooth、ZigBee などを介した家庭内の無線 LAN である。家庭内の他のメディア機器、プリンタ、PC、家庭内小型スイッチなどとの接続が想定される。

(4) インターネット接続

① 特定サイト接続　　　＜→　D1＞

特定サイトもしくは、特定サイトを介したサイトにのみ接続が可能なインターネット接続機能である。

② 任意サイト接続　　　＜→　D2＞

通常の PC と同じように、任意のサイトに接続が可能なインターネット接続機能である。サイトのフィルタリングは、接続プロバイダから提供されるフィルタリングサービス等を利用することになる。
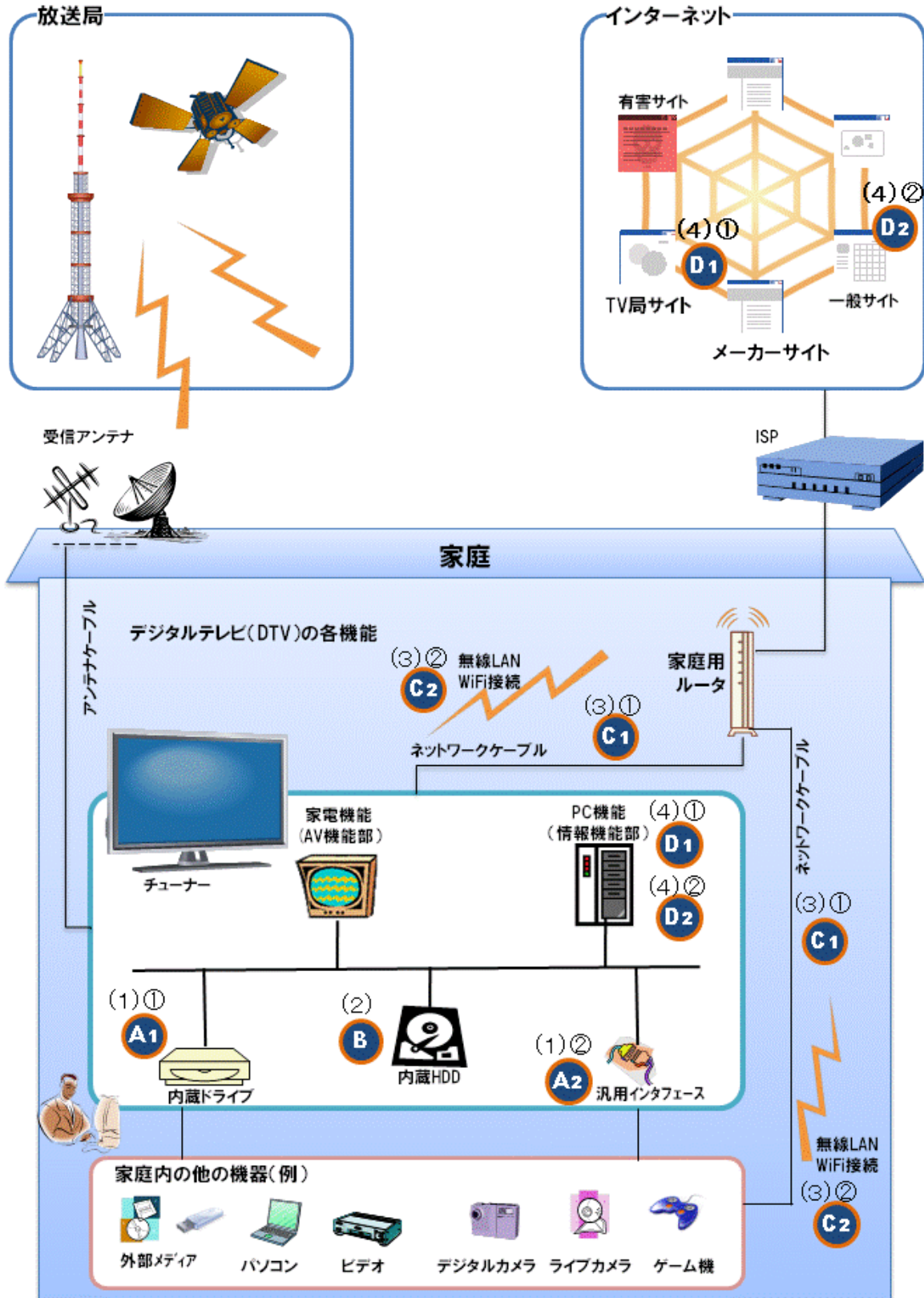
図1 デジタルテレビの構成概念図

(注) (n)○ は、3.1節の項番を、Ⓐ1～Ⓓ2は、3.1節表2左下の機能レベルの項番に対応

3.2　デジタルテレビに想定されるセキュリティ上の脅威

図２に、機能の全体構成図における想定脅威の一覧を示す。

情報利用機能が追加されていくと、発生する脅威は、PC およびそのインターネット接続で発生する脅威と、同じものが想定される。なお、脅威としては、一次的に発生しうる脅威を挙げることとする。従って、不正アクセスや盗聴の脅威が発生し、それが原因で二次的に起こりうる情報漏えい等は一次脅威としては含んでいない。

脅威群を、媒体利用、ユーザ操作、宅内、ネット経由　など、原因となる利用機能および場所で分類して、脅威群を列挙する。

(1)　媒体利用における脅威

①　ウイルス感染

媒体内のコンテンツに混入したウイルスや悪意あるソフトウェア（マルウェア等）などによる感染である。

(2)　ユーザ操作上における脅威

機器の利用サイクルにおけるユーザの操作（廃棄も含む）に起因するものとして以下が挙げられる：

①　設定不良

無線 LAN の利用、ネットの利用などで、セキュリティ上のパラメータなどが正しく設定されてないケースなど、それが原因で盗聴や不正アクセスの脅威が増す。

②　操作ミス

利用可能な機能の操作上のミスで、情報の漏えい（メールの誤送信や情報の誤送付）などの事故が発生するケースなどである。

③　蓄積情報の漏えい（コンテンツ）

デジタルテレビ内に利用者によって蓄積されたコンテンツの漏えいである。漏えい経路として、機器やネットを介した不正アクセス、ネットを経由した外部への送付、機器廃棄時の蓄積情報の残留（未消去）などが挙げられる。

④　蓄積情報の漏えい（ユーザ情報）

デジタルテレビ内に蓄積された、ユーザ個人に属する情報の漏えいである。この情報としては、個人情報（個人を特定できる情報）、機密情報（ID、Password など秘匿したい情報）、プライバシー情報（個人の機器の操作履歴やサービスの利用履歴を含む、個人に属する情報）など、機器に蓄積された、ユーザの操作や利用によって生成される全ての情報を含む。漏えい経路としては、③と同様である。
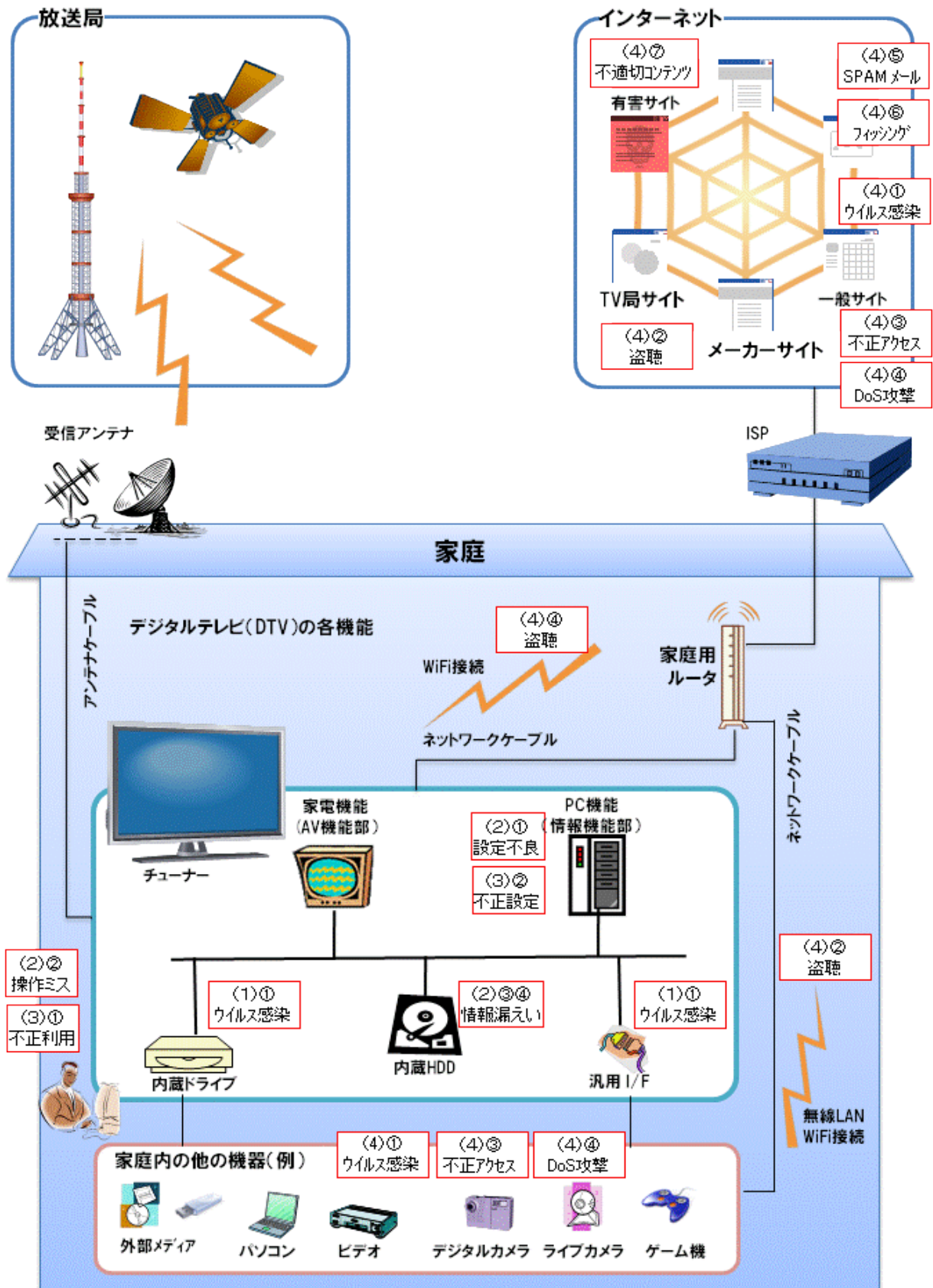
図2 デジタルテレビにおける脅威の全体像

(注1) (n)○ は、3. 2節の項番を指している。
(注2) スペースが限られており、該当箇所に全ての脅威を記載していないので、詳細は表2を参照の事。

(3) 宅内における脅威

① 不正利用（なりすまし）

宅内での、正規の利用者以外の者の利用である。同居している家族だけでなく、不正侵入した人間のケースもありうる。

② 不正設定

宅内への侵入、もしくは修理時等に、ユーザの意図に反した設定やプログラムがインストールされるケースなどである。

(4) ネット経由・ネット利用時

① ウイルス感染

メール利用、外部サイトのアクセス、コンテンツのダウンロードなどによって起るウイルス感染である。

② 盗聴

DTV から宅内の他の機器との通信や、DTV と外部の Web サーバや放送局との通信の情報が盗み見や奪取される脅威である。

③ 不正アクセス

ポートスキャン、脆弱性を狙った攻撃、なりすましなど、情報奪取やシステム破壊などを目的に行われる攻撃である。

④ DoS(Denial of Service)攻撃

不正な接続要求によってアクセス負荷（リクエスト要求）を高めることにより、正規のサービスの阻害やシステムダウンを狙った攻撃である。

⑤ スパム（SPAM）メール

ネット接続でメール機能を利用時に、悪意ある、もしくは利用者にとって不要なメールを送りつけられる脅威である。ネット利用効率の低下だけでなく、ウイルス感染やフィッシング詐欺の２次的な脅威の原因ともなる。

⑥ フィッシング

Web サービスの利用時に、正規のサービスサイトに成りすまして、利用者に使わせる脅威である。機密情報の奪取やウイルス感染を起こさせることを目的にしており、⑤のメールなどを経由して誘導されるケースが多い。情報家電の利用者として、老人や子供が操作するケースも考えられ、PC におけるより被害に合う可能性が高いことが懸念される。

⑦ 不適切コンテンツのアクセス

利用者が望んでいないコンテンツ（猥褻画像など）の表示や、家族が不用意に不適切なコンテンツにアクセスできてしまうなど、情報家電としての脅威である。

(5) ポータルサイト側

DTV 機器自体ではなく、機器にサービスを提供するサイト側（メーカー等が運営）の脅威

である。ただ、そこに接続する DTV 側に対しても、汚染や改ざんサイトとして間接的な脅威となる。

① 端末／ユーザの成りすまし

接続してきた端末の成りすまし、およびユーザの成りすましの脅威である。端末の成りすましは、サイトへの攻撃などの脅威となり、また、ユーザの成りすましは提供するサービスやコンテンツの不正利用の脅威となる。

② 一般 Web と同等脅威

サービスプロバイダ、Web サービスであるので、DoS 攻撃、不正アクセス、ウイルス感染、盗聴、SPAM メール、フィッシングなどの脅威がある。また、Web アプリケーションの脆弱性をついた攻撃（クロスサイトスクリプティング、SQL インジェクションなど）も、ウイルス感染や情報漏えいなどを引き起こす脅威となる。

3.3　脅威に対するセキュリティ対策

DTV に対する様々な脅威に対して、以下のセキュリティ対策群が挙げられる。

＜→：表２上半分左欄の項番に対応＞

(1) 脆弱性（セキュリティパッチ）対策　　　＜→　１＞

機器にインストールされている OS、ミドルウェア、アプリケーションに、脆弱性のパッチをあてる対策です。対象箇所として、DTV に対しては、主に

・家電機能（AV 機能部）

・PC 機能（情報機能部）

がある。そのパッチの入手とあて方については、放送波経由による方法や、インターネット接続サービスを経由する方法などがある。放送波経由では、深夜などのユーザが放送を利用していない時間帯での配信となる。インターネット接続サービスでは、特定の Web サイトの利用では、接続時にアップデートの必要性をアナウンスしてアップデートサービスの選択を誘導したり、アップデートをしないと先のサービスに進めない仕様にするなどが考えられる。

(2) ファイアウォール（FW）　　　＜→　２＞

DTV 側での対策としては、以下の２通りが挙げられる。

① 接続先特定（ルート制御）

接続先が特定されているインターネットサービスでは、その特定の IP アドレスとの通信のみを許可する設定とする。

② 不正アクセス防御

利用できるサービス（ポート）のみの利用にフィルタリングで制限する。

(3) アンチウイルス　　＜→　３＞

メディア経由でのウイルス感染、ネット（家庭内 LAN、インターネット双方）経由でのウイルス感染を防止する。パターンファイルの更新に関しては、インターネットに接続されているケースは PC と同様にネット経由で実現する。

(4) IDS／IPS（Intrusion Detection System／Intrusion Protection System）　＜→　４＞

不正アクセスや攻撃を、シグナチャベースやルールベースで検知／防止する。インターネット接続時に、通常の PC に対するクライアントセキュリティツールの利用が考えられる。シグナチャやルールの更新に関しては、インターネットに接続されているケースは PC と同様にネット経由で実現する。

(5) 通信路暗号化（VPN(Virtual Private Network))含む）　　＜→　５＞

通信路の暗号化の対象として、

① DTV 機器と宅内機器の有線／無線でのネット経由での情報のやり取り

② DTV 機器と、インターネットを介した外部 Web サービスとの情報のやり取り

③ DTV 機器を使った外部との情報のやり取り
が考えられる。

①に関しては、有線の場合は宅内配線とのことで、通常の家電同様に盗聴のリスクは低いと想定されるが、無線 LAN の利用時は、宅外からの盗聴を想定し、無線 LAN 機能に内蔵された暗号化機能を利用することが考えられるが、暗号強度の高い方式を採用すべきである。無線 LAN 機能を提供する場合は、その事を取扱い説明書で記載することが重要となる。

②に関しては、通常、SSL/TLS (Secure Socket Layer/ Transport Layer Security)のようにサービスサーバ側の暗号化機能で通信路を保護するのが一般的である。

③に関しては、メール等を用いた情報の授受などが想定されるが、これは、通常の PC での対策に準じることになる。利用者によって、送出される情報自体の暗号化や、暗号メール機能（S/MIME (Secure / Multipurpose Internet Mail Extensions)、PGP (Pretty Good Privacy) 等）を利用する事が考えられる。

(6) 認証

① 機器認証　　　＜→　6＞

DTV 機器自体の認証機能である。主に、情報サービス側が、接続してきた DTV 端末が正当なものであることを認証するために用いる。実現手段として、DTV 機器固有の ID や、機器に外部から装着された USB キーや IC カードなどを用いたり、機器に埋め込まれたチップ (TPM (Trusted Platform Module)) 等を用いることが考えられる。ID は成りすまされる脅威があり、端末機器自体を認証していることにはならない場合がある。

② ソフトウェア認証　　　＜→　7＞

DTV 機器にインストールされるソフトウェアの認証機能である。後付けで DTV に追加されるソフトウェアが、正当なものであるかを認証するために用いる。悪意のあるソフトウェアや、搭載が認められていないソフトウェアのインストールを防止するための機能である。プログラムに電子署名をするなどして、実現される。厳密な認証には、PKI (Public Key Infrastructure)を用いた電子署名が考えられる。

③ ユーザ認証（対機器）　　　＜→　8＞

DTV 機器を使用するユーザの認証である。DTV の不正利用抑止や、外部ソフトのインストールなどの特別な操作をする際に、ユーザ認証が重要となる。宅内の利用機器であるので、ID/PW を用いるのが一般的である。

④ ユーザ認証（対サービス）　　　＜→　9＞

DTV 機器を使用して、外部のネットサービスを利用する際のサービス側によるユーザ認証である。サービス側がどのような手段を選択するかによるが、一般的には、登録された ID/PW や、契約や購入が含まれるサービスでは、クレジットカード情報や、固有のデバイス（ワンタ

イム PW 生成機器）が用いられるケースや PKI の利用が考えられる。一般的な PC における
ネットサービス利用時と同じ状況となる。

⑤ サーバ認証（対接続サーバ）　　＜→　10＞

特定サイトサーバや放送局サイトサーバとの接続を確実に保証することが必要である場合、サーバ認証を実施する。これは、該当するサイトのサーバ証明書を DTV 機器側にプリインストールしておくことにより実施する。ソフトウェアや重要な情報のやり取りが必要なサービスに使用されることが考えられる。

(7) コンテンツ暗号化　　＜→　11＞

蓄積情報に対する暗号化機能である。蓄積される著作権のあるコンテンツやユーザ情報などが対象となる。暗号化の際、暗号鍵およびその管理方法も、対策内容を決める上で重要となる。

(8) データ消去ツール　　＜→　12＞

蓄積情報の消去機能である。対象は HDD、Flush メモリの双方となる。DTV 機器の廃棄時に、廃棄機器を介して情報が漏えいすることを抑止する。データ消去には、乱数の上書き（多数回）、ディスク等の破砕、磁気消去などあるが、家電機器では、乱数の上書きが一般的である。

(9) フィルタリングツール

① Web フィルタリング　　＜→　13＞

インターネット接続で、Web サービスが提供される場合に、外部からくるダウンロードされる情報のフィルタリング機能である。フィルタリング対象としては、不適切サイトへのアクセス、汚染サイトへのアクセスなどである。フィルタリングは URL のデータベースを用いて実施されるのが一般的である。　本機能は、DTV 機器自体に備わっているのではなく、ネットサービスの 1 メニューとして用意されることになる。

② メールフィルタリング　　＜→　14＞

インターネット接続で、メールサービスが提供される場合に、外部からくるメールのフィルタリング機能である。フィルタリング対象としては、SPAM メール、フィッシングメール、感染物の同梱メールなどである。　本機能は、DTV 機器自体に備わっているものではなく、ネットサービスの 1 メニューとして用意されることになる。

なお、内部から外部に送られるメールに対しては、情報漏えいなどが考えられるが、家電用途で用いられるケースでは PC と同じように対策はなされていない。

(10) 取扱い説明書明記　　　　　＜→　15＞

DTV の取扱い説明書に、利用開始から、運用、廃棄のライフサイクルに沿って、想定される脅威や事故の対応方法：

・誤使用の回避

・機能の選択

・セキュリティパラメータの設定

・セキュリティの運用（脆弱性対策など）

・機器異常時、故障時、事故時の対応

・廃棄時の対応

を機器のライフサイクル（利用開始、運用、廃棄）に沿って、想定される脅威や対応方法を記載することにより、想定される脅威の低減や、利用時の問題解決を図れる誘導をする。

3.4　情報利用機能、想定脅威、セキュリティ対策の相関一覧

前３節で挙げた、情報機能、想定脅威、セキュリティ対策に対して、その相関の一覧を表２に示す。

表の構成の各軸は以下である：
① 左下半分の縦軸に情報機能群を列挙している
② 中央左右の横軸に、脅威群を列挙している
③ 左上半分の縦軸に、対策群を列挙している

デジタルテレビに搭載される情報機能（①）から始めて、その機能に想定される脅威（②)、その脅威に対する対策（③）の相関を次の記載で示している：
・機能と脅威のマトリックス（表２の下半分）では、該当機能の搭載で想定される脅威として、
〇：発生する可能性が高い、△：発生する可能性は低い、空欄：発生する可能性はない、
ことを示している。
・脅威と対策のマトリックス（表２の上半分）では、該当脅威に対して対策として、
〇：対策として有効、△：対策として一部有効、空欄：該当脅威の対策でない、
ことを示している。
以下では、表２の情報機能 → 想定脅威と、想定脅威→ 対策のそれぞれにおける〇、△の考え方について説明する。

(1)　情報機能 → 想定脅威　　　（＜　＞は表２の機能の項番を、下線は脅威項目を指す）

基本機能は、従来のテレビ機能（映像受信、表示機能、利用管理機能等）を指している。これに対しては、設定不良、操作ミス、ユーザ操作によって生成された履歴ログや個人情報などのユーザ情報の漏えい、宅内における不正設定が、想定され、該当欄に〇を付している。
以下、3.1 節で挙げた情報機能に対して、想定される脅威を説明する。

① 外部メディア利用／内蔵ドライブ　　＜Ａ１＞

内蔵ドライブを経由して、DVD、ブルーレイ等の外部メディアの利用が行われる。その際、内部に取り込まれるコンテンツからのウイルス感染、内部のコンテンツの外部メディアへのコピーによる蓄積情報の漏えいが、脅威として挙げられる。

② 外部メディア利用／汎用インタフェース　　＜Ａ２＞

USB などの外部メディア利用や、他の AV 機器の接続を介して、内部に取り込まれるコンテンツからのウイルス感染、内部のコンテンツの外部メディアへのコピーによる蓄積情報の漏えい、汚染された装置との接続によるウイルス感染、DoS 攻撃、不正アクセスが、発生する可能性が挙げられる。

表2.　デジタルテレビの機能レベルに応じた脅威／対策一覧

○：対策として有効、 △：対策として一部有効、（空欄）：該当脅威の対策でない

No.	対策 ＼ 脅威（一次的） ／ 機能		媒体：ウイルス感染	ユーザ操作：設定不良	ユーザ操作：操作ミス	ユーザ操作：蓄積情報漏えい：コンテンツ	ユーザ操作：蓄積情報漏えい：ユーザ情報	宅内：不正利用（なりすまし）	宅内：不正設定（侵入、保守時等）	ネット経由：ウイルス感染	ネット経由：盗聴（ネット利用時）	ネット経由：不正アクセス	ネット経由：DoS攻撃	ネット経由：メール（SPAM）	ネット経由：フィッシング	ネット経由：不適切コンテンツアクセス	ポータルサイト側：端末／ユーザ成りすまし	ポータルサイト側：一般Webと同等脅威	備考
15	取扱い説明書明記			○	○	○	○				○ 無線LAN向け								
14	フィルタリングツール	メール向け												○	○ メール			○	プロバイダサービスとして提供
13	フィルタリングツール	URL 向け								○					○ サイトアクセス	○		○	プロバイダサービスとして提供
12	データ消去ツール					○ disk	○ flush												flushメモリ ／ Disk それぞれ
11	コンテンツ暗号化					△	△					△						○	
10	認証	サーバ（接続先）								△					○	△		○	
9	認証	ユーザ（対サービス）				△ ネット経由	△	○	○							△	○	○	サービス側におけるユーザ認証
8	認証	ユーザ（対機器）				○	○	○	○							△			機器の利用（ログイン）におけるユーザ認証
7	認証	ソフトウェア	○							○									機器にインストールされるソフト（ドライバ含む）の認証
6	認証	機器										△					○		サービス側の接続要求機器認証。機器ID，TPMなど
5	通信路暗号化（VPN含む）										○							○	Webサイト、プロバイダサービスとして提供
4	IDS/IPS									△		○	○					○	仮想パッチでウイルスにも対応
3	アンチウイルス		○							○								○	
2	ファイアウォール											○	○					○	ポート制御、接続先特定など
1	脆弱性（セキュリティパッチ）対策		○							○		○						○	衛星配信、もしくは、端末操作
	基本機能（デジタルTV機能）			○	○		○		○										
A1	外部メディア利用	内蔵ドライブ	△			○													DVD等のオプティカルドライブ
A2	外部メディア利用	汎用インタフェース経由	△			○				△		△	△						USB, Ethernet(IP)など
B	蓄積メディア内蔵					○	○												内蔵ハードディスク
C1	LAN	有線								△	△	△	△						機器間のケーブル接続
C2	LAN	無線		○						△	○	△	△						家庭内Hubルータ間
D1	インターネット接続	特定サイト		○	△	△ ネット経由	△ ネット経由	△	△	△	○	△	△	△	△	△	○	○	特定サイト側で対策してリスク低減
D2	インターネット接続	任意サイト		○	△	○ ネット経由	○ ネット経由	○	△	○	○	○	○	○	○	○	ー	ー	

○：発生する可能性が高い、 △：発生する可能性がある、（空欄）：発生可能性はない　　（網掛け）：該当せず

③ 蓄積メディア内蔵　＜B＞

蓄積メディアには、大量のコンテンツやユーザ情報の蓄積がなされる。そのデータに対する不正アクセスや廃棄時の消し忘れによって、蓄積情報の漏えいが挙げられる。

④ LAN　有線、無線　＜C１、C２＞

LAN の利用においては、汚染された他の家電機器や PC とのネット接続によるウイルス感染、DoS 攻撃、不正アクセス、盗聴が、発生する可能性が挙げられるが、宅内の機器や配線からの脅威としては、余り可能性は高くないものと考えられる。　但し、無線 LAN の利用に関しては、外部（宅外）に漏れる電波の盗聴は充分に想定される脅威であり、また、その利用にあたっての設定不良（プロトコル選択やセキュリティパラメータ設定）も大きな脅威となるため、無線 LAN の欄には、両者に○を付している。

⑤ ネット接続／特定サイト　＜D１＞

ユーザ操作では、家庭内 Hub への接続（無線含む）からネットサービスの利用において、設定不良、操作ミス、蓄積情報のネット経由での情報漏えいが挙げられる。設定不良は無線 LAN の利用も想定して○を、他は、ネット接続先および提供ネットサービスが限定されることから△としている。

宅内では、不正利用、不正設定が挙げられるが、両者とも脅威発生は高くないと考えられる。

ネット経由では、PC でのインターネット利用と同じ脅威が起こることが想定される。ウイルス感染、サーバ機能利用時の DoS 攻撃、不正アクセス、盗聴、メール（SPAM)、フィッシング、不適切コンテンツアクセスが挙げられる。但し、ネット接続先および提供ネットサービスが限定されることから、盗聴を除いては、△としている。盗聴に対しては、インターネット利用で通常起りうるため、○としている。

接続サービスを提供するポータルサイト側では、端末／ユーザの成りすましや、インターネットでサービスを提供しているため、一般の Web と同等の脅威が想定される。サービス提供者としての脅威群であるが、後者の一般の Web と同等の脅威への対策の不備は、接続してくる DTV 機器側に対しても間接的な脅威となるので、充分な対策がなされていないと、前段の DTV 機器側の脅威レベル（△）が保証されなくなる恐れがある。

⑥ ネット接続／任意サイト　＜D２＞

任意サイトのネット接続においても、想定される脅威項目は、⑤と同様である。但し、接続先やネットサービス範囲が広がることで、脅威の発生する可能性は高まり、蓄積情報漏えいと、ネット経由での脅威項目の全ての脅威項目が⑤での△から○となる。

(2)　想定脅威→ セキュリティ対策　（「　」は表２の対策の項番を指す）

① 媒体経由ウイルス感染

媒体からダウンロードされるウイルスが付着したコンテンツや悪意をもったソフトウェアに対して、ウイルスに対するアンチウイルスソフト「３」、ウイルスやマルウェアの活動被害を受けないための脆弱性対策「１」、ソフトウェアのインストールにあたって正規のものであることを確認するソフトウェアの認証「７」が挙げられる。

② ユーザ操作／　設定不良、操作ミス

設定不良、操作ミスに対しては、利用者の適切なガイドや利用者のリテラシーの向上を達成するため、取扱い説明書に分かり易く明記「15」することが重要となる。

③ 蓄積情報漏えい／　コンテンツ、ユーザ情報

蓄積情報漏えいに対しては、情報のアクセス制御や保護と、適切な消去処理が挙げられる。

前者に対しては、機器操作で情報にアクセスできるユーザの認証「８」、不正にアクセスされた場合でも情報自体を保護するコンテンツの暗号化「11」が挙げられる。また、外部に情報を送付されることを抑止するため、サービスを利用できるユーザの認証「９」が挙げられる。

後者に対しては、機器の廃棄時の蓄積情報のデータ消去ツール「12」と、廃棄時にユーザがすべきこと（データ消去ツールの利用など）を取扱い説明書に明記「15」することが挙げられる。データ消去ツールに対しては、情報格納場所が HDD や Flush メモリに散在する場合は、その双方の消去ツールを備えることが必要となる。

④ 宅内／　不正利用、不正設定

宅内における不正使用や不正設定は、操作するユーザを適切に認証する機能により対策する。機器の機能利用におけるユーザ認証「８」、ネット等のサービス利用におけるユーザ認証「９」が挙げられる。後者は、サービス提供するサイト側の機能となるが、ID／パスワードではなく、デバイス等を前提とする場合は、機器側に、そのデバイスを入力できる機能が必要となる。

⑤ ネット経由／　ウイルス感染

ウイルスが付着したコンテンツやメールに対して、ウイルスに対するアンチウイルスソフト「３」、ネット経由のウイルスからの攻撃パケットに対して脆弱性対策「１」と、IDS/IPS「４」が挙げられる。「４」は、パターンファイルが間に合わないウイルスからの攻撃や、亜種のウイルス対策にもなりうる。

ソフトウェアのダウンロードにあたっては正規のものであることを確認するソフトウェアの認証「７」が、また接続先の脅威を低減する対策として、接続先サーバの認証「10」、汚染の危険性が高いサイトへの接続を回避する URL 向けフィルタリング「14」が挙げられる。

⑥ ネット経由／　DoS 攻撃

DoS 攻撃に対しては、提供するサービスポートやパケットをフィルタリングするファイアウォール「２」、不正パケットを検知、廃棄する IDS/IPS「４」が挙げられる。攻撃元が特定さ

れている場合には、「２」「４」の連携で、不正パケットの廃棄が可能だが、不特定多数からの場合には、対策が困難である。ただ、個人のサーバ機能向けに DDoS (Distributed Denial of Service)攻撃がくる可能性は低いものと考えられる。

⑦ ネット経由／　不正アクセス

不正アクセスに対しては、サービスポートやパケットをフィルタリングするファイアウォール「２」、脆弱性対策「１」、不正パケットを検知、廃棄する IDS/IPS「４」が挙げられる。また、不正アクセスがされてしまった場合に、情報を保護するコンテンツ暗号化「11」が保険的な対策として挙げられる。なお、LAN 接続においては、接続される機器の認証「６」を行うことも考えられるが (MAC(Media Access Control address)認証他)、家庭内で行われるのは余り一般的ではないものと考える。

⑧ ネット経由／　盗聴

ネット経由の盗聴の対策としては、通信路暗号化「５」が挙げられる。通信路暗号化は、区間、手段でバリエーションがある（3.3(5)参照）。また、無線 LAN 使用時の暗号方式選定にあたっては、取扱い説明書での明記「15」が必要である。なお、無線 LAN の暗号強度の設定では、デフォルトを強度の高いものとする考慮も必要である。

⑨ ネット経由／　メール（SPAM）

メールサービス利用における SPAM メールは、ウイルス感染、フィッシングなどの間接的な原因ともなる。メール向けのフィルタリング「13」が対策として挙げられるが、プロバイダサービスの一つとして提供されるのが一般的である。

⑩ ネット経由／　フィッシング

フィッシングに対する対策として、ユーザ自身が、接続先の URL を DTV 上で確認することが基本的な対策となるが、それを省略したり、すり抜けたりする脅威に対して、リスクを下げるための対策が何種類か用意されている。

まず、フィッシングの契機となる SPAM 等のメールのフィルタリング「13」が挙げられる。また、アクセスするサイトに対して、ブラックリストに載っているサイトでないかを検証する URL のフィルタリング「14」や、接続先サイトのサーバの認証「10」が挙げられる。これらは、プロバイダサービスの一つとして提供されるのが一般的である。

⑪ ネット経由／　不適切コンテンツアクセス

本人や家族の不適切コンテンツアクセスに対する対策としては、まず、機器やサービスを使うことを制御する、機器へのユーザ認証「８」、サービスへのユーザ認証「９」が挙げられる。また、不用意にそうしたサイトにアクセスすることを抑止する対策として、接続先サーバの認証「10」や、URL 向けのフィルタリング「14」が挙げられる。

⑫ ポータルサイト側

ポータルサイトとしては、一般の Web サービスにおいてなされているセキュリティ対策を表２に示した。なお、本表に含んでいないものとして、以下が挙げられる：

・Web アプリケーションの脆弱性攻撃に対する WAF（Web Application Firewall）[8] の活用

・サービスの可用性を確保するためのシステムの冗長構成

3.5　製品設計における活用方法　<テンプレート、チェックリスト>

前節で述べたように、表２の一覧表を用いて、対象のデジタルテレビに搭載している情報機能に対して、横方向に想定される脅威を抽出し、その脅威に対して、縦方向に対応するセキュリティ策を抽出することが可能である。

その活用方法として、

・セキュリティ対策のテンプレートとして用いるケース

・製品のセキュリティ機能のチェックリストとして用いるケース

の２通りが考えられる。

(1)　商品の企画、設計時のセキュリティ対策のテンプレート

商品の企画、設計時において、どのようなセキュリティ対策機能を実装する必要があるかを検討するテンプレートとして用いる。

該当商品に搭載する機能欄だけを残し、その機能に対する○△のついた脅威に対する対策として、縦方向に○△のついた対策を抽出する。

各○△のついたセキュリティ対策に対して、どのような対策機能を搭載するのか、あるいは該当製品には脅威は小さいと判断して対策機能搭載をしないかなどを、検討する。なお、抽出した脅威や対策の具体的な内容については、それぞれ、3.2 節、3.3 節で記載しているので、それを参考に、実際の対策機能を決定する。

(2)　現製品のセキュリティ機能のチェックリスト

現製品に搭載している情報機能に該当する脅威と対策項目に対して、どのようなセキュリティ対策がなされているかを、○△のついた項ごとにチェックする。各項目に対して、該当製品に対応セキュリティ機能がある場合はその対策レベルを、あるいは、セキュリティ機能がない場合はその妥当性を検証する。

なお、本表（またはその加工版）を、取扱い説明書に添付することにより、DTV の利用者（購入者）に、該当製品の情報機能を利用するにあたって想定される（留意しなくてはならない）脅威の理解（説明）や、搭載しているセキュリティ対策の認識（確認）を図るために用いることが考えられる。また、取扱い説明書の中で、脅威やセキュリティ対策の記載箇所を、容易に見つけるための一覧（索引）として用いることなどが挙げられる。利用者にとって、
脅威やセキュリティ対策の説明や情報を、より分かり易い形で提示することが重要であると考える。

3.6　補遺

本報告書では、情報家電およびDTVを全般的(個別商品の仕様や特定機能に非依存)に捉え、想定される脅威とセキュリティ対策を纏めることとした。ただ、勉強会の中で、意見で出た事項で、検討を要する事項について、以下に述べる。

(1)　DTV機器のシステム構成（構造）の観点

情報家電共通の課題であるが、デジタルテレビも、AV系（家電機能）と情報系（PC機能）が共存していることによって、それぞれの部位に対して、

・ユーザに必要とされるリテラシーレベルの違い　（セキュリティ意識や操作ノウハウなど）
・製品寿命に対する期待値の違い　（一般的に家電は10〜15年、PCは5年程度）
・さらされるセキュリティ脅威レベルの違い

などをどう救済、解決していくのかが、重要な課題となってくる。　2.1節で述べた懸案、隘路の多くが、ここに起因している。従って、ここをどう分離していくかが一つの解決の方向性ではあるが、逆に、「情報家電」としての便利な機能や使い勝手やコスト面とのトレードオフになることになる。

3.3節、3.4節で挙げたセキュリティ対策は、セキュリティ機能の追加や外付けでできる対策事項を挙げた。ただ、上述のように、デジタルテレビ自体の作り（構造）による対策も一つの本質的な選択肢である。AV系と情報系のシステムの論理的な分離などにより、AV系に対するセキュリティ脅威の低減がはかられる。ただ、それはデジタルテレビの機能やサービスのレベルに大きく依存するため、個別の製品の機能に関わることもあり、本報告書では言及しないこととした。

(2)　デジタル放送利用における脅威の対策

デジタル放送のサービスにおいて、配信先、授受情報含め、どの程度の脅威を想定しておく必要があるのか現時点では不明のため、3.3節、3.4節で挙げたセキュリティ対策には含んでいない。用途と脅威として以下が挙げられる：

・データ放送利用時

データ放送で下りてくる情報の中に、スクリプトなどの実行が含まれた場合、そのスクリプトによる不正行為や攻撃の可能性。

（３）デジタルテレビにおける脅威の検証

前節までは、PCと同じような情報利用機能やネット利用機能がデジタルテレビに備えられることで想定される脅威を挙げて議論した。しかし、デジタルテレビの機器自体を構成しているプロセッサやOSやライブラリ群は、現在のPCとは異なっており、必ずしもPCと同じ脅威が発生する訳ではない。ただ、プロセッサもかなり知られたチップの利用や、アンドロイドといったオープンなプラットフォームの採用などによって、攻撃コードを作るハードルは年々

低くなってきていることも事実である。

　そうしたことを踏まえた脅威の検証、および脅威の大きさの観点も加えた対策を検討していくことが必要である。

＜参考文献＞

1】　IPA 公開ホームページ／情報セキュリティ／脆弱性対策、
http://www.ipa.go.jp/security/vuln/index.html

2】　組込みシステムのセキュリティへの取組みガイド（改訂版）、 情報処理推進機構、
http://www.ipa.go.jp/security/fy22/reports/emb_app2010/index.html, (2010.9)

3】 組込みソフトウェアを用いた機器におけるセキュリティ、情報処理推進機構、
http://www.ipa.go.jp/security/fy17/reports/vuln_handling/documents/2_kiki.pdf, (2006.8)

4】　JVN iPedia ホームページ, 情報処理推進機構、　http://jvndb.jvn.jp/

5】　MyJVN ホームページ, 情報処理推進機構、http://jvndb.jvn.jp/apis/myjvn/

6】　JCB グローバルサイト PCI データセキュリティスタンダード「PCI DSS」、
http://www.jcb-global.com/pci/index.html

7】　情報セキュリティ早期警戒パートナーシップガイドライン、
http://www.ipa.go.jp/security/ciadr/partnership_guide.pdf

8】　Web Application Firewall 読本、情報処理推進機構、
http://www.ipa.go.jp/security/vuln/documents/waf.pdf, (2010.10)

IPAの提供するセキュリティ関連コンテンツ

IPAセキュリティセンターでは、情報セキュリティ対策の普及啓発活動の一環として、以下のようなコンテンツを提供しています。是非ご活用ください。

●: ユーザ向け　▲: 開発者向け　◆: 経営者向け

情報セキュリティ対策ベンチマーク▲◆
組織の情報セキュリティマネジメントシステムの実施状況を自らが評価する自己診断ツールです。40の設問に答えることでセキュリティに関する自社の取組みがどの程度のレベルにあるのか分かります。
http://www.ipa.go.jp/security/benchmark/index.html

iLogScanner●▲
ウェブサイトのアクセスログを解析することで、そのサイトへの攻撃痕跡を確認するツールです。運営しているウェブサイトがどれほど攻撃を受けているか等の状況を把握することができます。
http://www.ipa.go.jp/security/vuln/iLogScanner/index.html

安全なウェブサイト運営入門●▲
ウェブサイトの脆弱性による被害を中心とした7つの具体的な事件を題材に、ロールプレイング形式で体験的に学習できるソフトウェアです。事件や事故が発生した場合の被害を理解し、事前対策の必要性を学ぶことができます。
http://www.ipa.go.jp/security/vuln/7incidents/index.html

知っていますか?脆弱性(ぜいじゃくせい)●▲
ウェブサイトの運営者や一般利用者向けに、ウェブサイトにおける代表的な10種類の脆弱性について、わかりやすくアニメーションで解説したものです。脆弱性についての理解を深めることができます。
http://www.ipa.go.jp/security/vuln/vuln_contents/index.html

JVN iPedia●▲
国内の製品開発者から公開された対策情報、および海外の脆弱性関連情報のデータベースに登録された情報に基づき脆弱性関連情報を網羅、蓄積しています。検索機能やRSS配信機能を利用することで効率的に脆弱性関連情報を収集することができます。
http://jvndb.jvn.jp/

MyJVN●▲
JVN iPediaに登録された脆弱性関連情報の中から、利用者が必要とする情報のみを効率的に収集できます。情報収集にかかる時間の節約だけではなく、適切な対策を素早く実施できるようになります。
http://jvndb.jvn.jp/apis/myjvn/

セキュリティ情報RSSポータル●▲◆
インターネット上に発信されている様々な情報から、セキュリティに関する最新情報を収集・整理し、セキュリティに関する情報を利用しやすく提供するシステムです。多数のWebサイト上に散在する最新情報を効率よく確認することができます。
http://www.ipa.go.jp/security/fy19/development/rss/

●: ユーザ向け　▲: 開発者向け　◆: 経営者向け

暗号技術に関するe-Learning教材▲
システムの選定や調達仕様の作成などに必要な暗号技術に関する知識を、幅広く修得するための教材です。ネットワークを通じて教育を行うので、時間や場所を選ばずに暗号技術に関する学習が行えます。
http://www.ipa.go.jp/security/fy19/development/e_Learning_Cipher/index.html

セキュアプログラミング講座▲
想定される様々な攻撃への対策として留意すべき事項を、ソフトウェア開発工程に沿って解説しています。セキュリティ対策を意識したプログラミングができるようになります。
http://www.ipa.go.jp/security/awareness/vendor/programmingv2/index.html

TCP/IPに係わる既知の脆弱性検証ツール▲
TCP/IP(Transmission Control Protocol / Internet Protocol) を実装したソフトウェアの脆弱性を体系的に検証し、自社で開発したソフトウェアに、既知の脆弱性が再び作り込まれないよう防止するためのツールです。TCP/IP利用機器の脆弱性の有無を簡易判定することができます。
http://www.ipa.go.jp/security/vuln/vuln_TCPIP_Check.html

SIPに係る既知の脆弱性検証ツール▲
SIP(Session Initiation Protocol)を実装したソフトウェアの脆弱性を体系的に検証し、自社で開発されるソフトウェアに既知の脆弱性が再び作り込まれないよう防止するためのツールです。
SIPを実装したソフトウェアの脆弱性の有無を簡易判定することができます。
http://www.ipa.go.jp/security/vuln/vuln_SIP_Check.html

ITセキュリティ評価・認証に関するe-Learning教材▲
ITセキュリティ評価・認証に関連する専門書を読みこなし活用するための入門的な教材です。「自己学習課題」に取組むことにより、習得した知識を実践に結び付け、実際のシステム開発に生かすことができます。
http://www.ipa.go.jp/security/fy19/development/e_Learning_CC/index.html

5分でできる！情報セキュリティポイント学習●▲◆
主に中小企業で働く方を対象とした、1テーマ5分で情報セキュリティについて勉強できる学習ツールです。あなたの職場の日常の1コマを取り入れた親しみやすい学習テーマで、セキュリティに関する様々な事例を疑似体験しながら正しい対処法を学ぶことができます。
http://www.ipa.go.jp/security/vuln/5mins_point/index.html

IPAでは今後も関係団体等と協力の下、セキュリティ対策の普及に向けた活動を継続していきます。
上記コンテンツ・報告書等へのお問い合わせ、ご意見がございましたら以下までお寄せ下さい。

IPAセキュリティセンター　isec-info@ipa.go.jp